IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JOANNE ROMA et al., individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **PROSPECT MEDICAL HOLDINGS, INC.,** **Defendant.**	**CIVIL ACTION** **NO. 23-3216**

OPINION

Defendant Prospect Medical Holdings, Inc. ("Prospect") moves to dismiss Plaintiffs' Amended Complaint, arguing that their lawsuit does not present a live case or controversy under Article III of the United States Constitution, and, in any event, they are not plausibly entitled to relief under any of the claims that they pursue. Fed. R. Civ. P. 12(b)(1), 12(b)(6). Plaintiffs have Article III standing, and they have stated a plausible claim for relief under only some—but not all—of the causes of action that they have identified, so Prospect's Motion will be granted in part and denied in part.

I. BACKGROUND

The below factual recitation is taken from Plaintiffs' Amended Complaint, well-pleaded allegations from which are taken as true at this stage. *Fowler v. UPMC Shadyside*, 578 F.3d 203, 210-11 (3d Cir. 2009).

A. Prospect Suffers a Data Breach and Notifies its Customers

Prospect is a medical group with over 18,000 employees and about 600,000 members that provides healthcare services at sixteen different hospitals across five states. "As a condition of providing medical care and billing" to Plaintiffs, Prospect received and stored patients' personally identifiable information ("PII") and protected health information ("PHI").

Early in the morning of August 3, 2023, Prospect reported a cyberattack to the Connecticut public health department. The company had detected unauthorized access to its network sometime over the four previous days. This data breach had exposed customers' "full names, Social Security numbers, addresses, dates of birth, driver's license numbers, . . . financial information[,] diagnosis information, lab results, prescription information, treatment information, health insurance information, claims information, and medical record numbers."

A ransomware gang called Rhysida took responsibility for the attack, posting a dataset with over one terabyte of customers' PII and PHI on the dark web. Rhysida said that this data included over half a million social security numbers, along with patients' medical files, passports, driver's licenses, and "financial and legal documents." Those files, and a related 1.3 terabyte SQL database, were for sale for fifty bitcoin (about $1.3 million). "[M]ore than half of the data," was sold, and another 45% was "leaked."

Starting on September 29, almost two months after the data breach had been discovered, Prospect began to notify state Attorneys General that it had been the victim of a cyberattack. One such notice letter, which is cited in the Amended Complaint,[1] includes a sample letter. In it, Prospect conceded that:

> While in our IT network, the unauthorized party accessed files that contain information pertaining to Prospect Medical employees and dependents. Our investigation cannot rule out the possibility that, as a result of this incident, files containing some of your information may have been subject to unauthorized access. This information may have included your name and Social Security number.

[1] "To decide a motion to dismiss, courts generally consider only the allegations contained in the complaint, exhibits attached to the complaint[,] and matters of public record." *Pension Benefit Guar. Corp. v. White Consol. Indus., Inc.*, 998 F.2d 1192, 1196 (3d Cir. 1993) (citations omitted). But "a document integral to or explicitly relied upon in the complaint may be considered without converting the motion to dismiss into one for summary judgment." *Doe v. Univ. of Scis.*, 961 F.3d 203, 208 (3d Cir. 2020) (quoting *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir. 1997)). As the notice letter is explicitly relied upon in the Amended Complaint, it can be considered in evaluating Prospect's Motion to Dismiss.

Prospect offered its customers free credit monitoring and identity protection services and encouraged them to "review[their] account statements and free credit reports for any unauthorized activity." The notice letter also provided information on how to set up (and lift) a fraud alert or credit freeze on one's credit report.

Plaintiffs allege that, "[b]ased on the type of sophisticated and targeted criminal activity, the type of Private Information involved, and [Prospect's] admission that the Private Information was accessed, it can be concluded that the unauthorized criminal third party was able to successfully target [their] Private Information . . . and exfiltrate" it "for the purposes of utilizing or selling [it] for use in future fraud and identity theft related cases."

B. The Named Plaintiffs' Responses to the Data Breach

The Amended Complaint is brought on behalf of a nationwide class (and a California subclass) led by several Named Plaintiffs each of whom received the notice but each of whose experiences following the data breach vary somewhat. They allege that not only do they face a "substantially increased risk of fraud, identity theft, and misuse" of their personal information, but they also have:

> spent time . . . on the telephone and sorting through [their] unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring [their] accounts.

They also "have suffered anxiety, emotional distress, [and a] loss of privacy." Six—but not all—of them allege that, since the data breach, they have seen evidence that unauthorized parties have tried to make financial transactions on their behalf:

1. Laura Doverspike: Doverspike's credit card has received fraudulent charges "from an entity called 'Midnight Wonders' that she has no affiliation with." These three charges totaled at least $139. She has been working to get these fraudulent charges reversed.

2. Rodney Hoggro: "[A]n unauthorized recipient of" Hoggro's PHI/PII has taken out student loans in his name. He "has never taken out any student loans."

3. Shamoon Khandia: Khandia has received notifications from the credit agency Experian "notifying him of charges on his . . . credit report that did not belong to" him. His credit score has gone down as a result, and he has moved his spending from his credit card to his debit card.

4. Fidel Medina: Medina "has received several letters in the mail informing him that he has been denied loans that he did not apply for (specifically card loans and credit card loans)." He "has over 27 hard inquiries on his credit report that he did not authorize. His credit score dropped over 200 points in September 2023."

5. Lorelei Phillips: Phillips found a $832 fraudulent charge on her Home Depot card. She also has received eight letters from entities like Synchrony Bank, Shell Oil, and Target "denying her from opening accounts that she did not authorize or attempt to open."

6. Latoya Pratcher: Pratcher has "experienced an unauthorized attempt to access a credit card account in her name" and has received more spam emails and phone calls than normal. She also has "obtained a report from Experian confirming that some of her compromised data has appeared on the dark web."

C. Procedural Background

The claims alleged by Plaintiffs are that Prospect's failure to safeguard their data: (1) breached its duty of care to them and thus constituted negligence; (2) violated Section Five of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, thus constituting negligence *per se*; (3) breached their implied contract with the company; (4) amounted to an intentional intrusion into matters in which they had a reasonable expectation of privacy; (5) violated the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56 *et seq.*; (6) violated the California Unfair Competition Act, Cal. Bus. & Prof. Code § 17200 *et seq.*; and, (7) violated Article I, Section 1 of the California Constitution, Cal. Const. art. I, § 1.[2] They seek both damages and injunctive relief, including a court order mandating that Prospect overhaul its information security practices.

The putative nationwide class consists of: "All persons in the United States whose

[2] The Amended Complaint also alleged violations of the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*, but Plaintiffs have withdrawn this count.

personal information was compromised in or as a result of Prospect's data breach on or around July 31, 2023 through August 3, 2023, which was announced on or around September 29, 2023." The putative subclass consists of: "All persons residing in California whose personal information was compromised in or as a result of Prospect's data breach on or around July 31, 2023 through August 3, 2023, which was announced on or around September 29, 2023." The alleged violations of California statutory and constitutional law are pressed on behalf of the California subclass only (all the Named Plaintiffs are citizens of California and are members of the subclass).

II. DISCUSSION

Prospect moves to dismiss the Amended Complaint on two grounds. First, the company argues that none of the Named Plaintiffs has standing to sue consistent with Article III of the United States Constitution. Fed. R. Civ. P. 12(b)(1). But each Named Plaintiff has plausibly alleged cognizable concrete and imminent injuries that confer them with standing, so Prospect's Motion will be denied in that regard. Second, the company argues that Plaintiffs have not plausibly alleged that they are entitled to relief under any of the common-law or statutory claims in their Amended Complaint. That is the case for some, but not all, of Plaintiffs' claims, so Prospect's Motion will be granted in part and denied in part in this respect.

A. Plaintiffs' Article III Standing

"Federal courts are courts of limited jurisdiction. They possess only that power authorized by Constitution and statute . . . ." *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994) (citations omitted). The United States Constitution limits "the judicial power of the federal courts . . . to 'cases' and 'controversies.'" *Flast v. Cohen*, 392 U.S. 83, 94 (1968); U.S. Const. art. III, § 2, cl. 1. For a lawsuit to satisfy that requirement, the plaintiffs must have standing to sue. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

Prospect argues that, because Plaintiffs lack Article III standing, the Court must dismiss the Amended Complaint for lack of subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). In evaluating such a motion, "[a] district court has to first determine . . . whether" it "presents a 'facial' attack or a 'factual' attack on the claim at issue." *Const. Party of Pa. v. Aichele*, 757 F.3d 347, 357 (3d Cir. 2014). "A facial attack, as the adjective indicates, is an argument that considers a claim on its face and asserts that it is insufficient to invoke the subject matter jurisdiction of the court . . . ." *Id.* at 358. "A factual attack, on the other hand, is an argument that there is no subject matter jurisdiction because the facts of the case—and here the District Court may look beyond the pleadings to ascertain the facts—do not support the asserted jurisdiction." *Id.*

Here, Prospect advances a facial challenge to the Court's jurisdiction, attacking the sufficiency of the allegations in the Amended Complaint. "In reviewing a facial challenge, . . . 'the court must only consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff.'" *In re Schering Plough Corp. Intron/Temodar Consumer Class Action*, 678 F.3d 235, 243 (3d Cir. 2012) (quoting *Gould Elecs. Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000)); *see Aichele*, 757 F.3d at 358.

"[T]o satisfy Article III's standing requirements, a plaintiff must show[:] (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and[,] (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[3] *Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000). Thus, the allegations in the Amended Complaint are

[3] Prospect attacks only the first two of these requirements, so redressability is not at issue here.

evaluated in light of these requirements. Where, as here, Plaintiffs press a class action, only one Named Plaintiff need have standing for the matter to proceed. *In re Horizon Healthcare Servs. Data Breach Litig.*, 846 F.3d 625, 634 (3d Cir. 2017). Conversely, "if none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974) (citations omitted).

i. Injury in Fact

An injury in fact is "an invasion of a legally protected interest which is (a) concrete and particularized, . . . and (b) actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560 (internal quotation marks and citations omitted). Both the actual injuries that Doverspike and Medina have suffered and the allegations of an ongoing risk of identity theft to every Named Plaintiff satisfy these requirements.

a. Actual or Imminent

An injury in fact must be actual or imminent. An actual injury is exactly what it sounds like: "a concrete loss as the result of [the defendant's] actions." *Taliaferro v. Darby Twp. Zoning Bd.*, 458 F.3d 181, 190 (3d Cir. 2006). In contrast, a future or imminent injury fits the bill only where "the threatened injury is 'certainly impending,' or there is a '"substantial risk" that the harm will occur.'" *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). "A substantial risk means a realistic danger of sustaining a direct injury." *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152-53 (3d Cir. 2022) (internal quotation marks and citation omitted). Thus, as the Third Circuit has observed:

> That 'actual or imminent' is disjunctive is critical: it indicates that a plaintiff need not wait until he or she has *actually* sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent. This

> is especially important in the data breach context, where the disclosure of the data may cause future harm as opposed to currently felt harm.

Id. at 152.

Two Third Circuit opinions provide a helpful taxonomy of the injuries typically alleged in data breach cases and when they can function as injuries-in-fact. In *Reilly v. Ceridian Corporation*, the plaintiffs, lawyers employed by a customer of the defendant, sued after they were notified that a hacker "may have . . . illegally accessed" their data, including their name, "social security number and, in several cases, birth date and/or the bank account that is used for direct deposit." 664 F.3d 38, 40 (3d Cir. 2011). "It [was] not known whether the hacker read, copied, or understood the data." *Id.* The *Reilly* plaintiffs alleged this data breach had led to "an increased risk of identity theft," "costs to monitor their credit activity," and "emotional distress," thus injuring them. *Id.* The Third Circuit held that they had not suffered an injury in fact because the plaintiffs:

> rel[ied] on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intend[ed] to commit future criminal acts by misusing the information; and (3) [wa]s able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.

Id. at 42. As pleaded, the future injuries alleged were "dependent on entirely speculative, future actions of an unknown third-party." *Id.*

These allegations stand in sharp contrast to those analyzed in *Clemens*. There, the defendant fell victim to a phishing scheme at the hands of a hacking group called CLOP, stealing "social security numbers, dates of birth, full names, home addresses, taxpayer identification numbers, banking information, credit card numbers, driver's license numbers, sensitive tax forms, and passport numbers." *Clemens*, 48 F.4th at 150. CLOP published this information on

the dark web, which, as alleged in that case, "is most widely used as an underground black market where individuals sell illegal products like . . . sensitive stolen data that can be used to commit identity theft or fraud." *Id.* Research had confirmed that employees' personal information in fact was for sale on the dark web. *Id.* In response, Clemens "conducted a review of her financial records and credit reports for unauthorized activity; placed fraud alerts on her credit reports; transferred her account to a new bank; enrolled in [the defendant's] complimentary one-year credit monitoring services; and purchased three-bureau credit monitoring services for herself and her family." *Id.* at 151. She rested her allegations of injury-in-fact on both "the risk of identity theft and fraud" and "the investment of time and money to mitigate potential harm."

The Third Circuit held that *Reilly* was distinguishable and allowed Clemens's lawsuit to proceed. *Reilly* had not "create[d] a bright line rule precluding standing based on the alleged risk of identity theft or fraud." *Id.* at 153. Instead, *Reilly* merely reflected the rule that an alleged future injury could not be hypothetical. In cases like this one, whether that is so turns on "non-exhaustive factors" such as: (1) "whether the data breach was intentional;" (2) "whether the data was misused;" and, (3) "whether the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft." *Id.* at 153-54.

In *Clemens*, these factors pointed in favor of treating the injuries alleged as sufficiently imminent to satisfy Article III. Clemens had identified "a known hacker group named CLOP [that had] accessed [her] sensitive information." *Id.* at 156. This injury was not hypothetical at all: "CLOP ha[d] already published Clemens's data on the Dark Web, a platform that facilitates criminal activity worldwide." *Id.* at 157. The Third Circuit could "reasonably assume that many of those who visit the Dark Web, and especially those who seek out and access CLOP's posts, do

so with nefarious intent," so "it follows that Clemens faces a substantial risk of identity theft or fraud by virtue of her personal information being made available on underground websites." *Id.* Moreover, CLOP's breach was intentional, and it misused Clemens's personal data by encrypting it, holding it for ransom, and publishing it. *Id.* (citations omitted). Finally, her "data was also the type of data that could be used to perpetrate identity theft or fraud" because it "contained social security numbers, dates of birth, full names, home addresses, taxpayer identification numbers, banking information, credit card numbers, driver's license numbers, sensitive tax forms, and passport numbers." *Id.* "Together, these factors" amounted to the necessary "'substantial risk that harm will occur' sufficient to establish an 'imminent' injury." *Id.* (quoting *Susan B. Anthony List*, 573 U.S. at 158).

Here, the future injuries that Plaintiffs identified share much in common with those analyzed in *Clemens*. Plaintiffs allege that, among other things, they have been injured because they have been subject to a "substantially increased risk of fraud, identity theft, and misuse resulting from [their] PII and PHI" having been "placed in the hands of unauthorized third-parties and possibly criminals." Left unsupported, this allegation could be construed as purely hypothetical and thus, per *Reilly*, insufficient to describe imminent injury. 664 F.3d at 42. But other allegations show that this future injury is not hypothetical at all. As in *Clemens*, Rhysida's theft of Prospect's data was intentional, and the data that was exposed—here, social security numbers, health information, and passport and driver's license information—although not identical to the data stolen in the Third Circuit's case, is "the type . . . that could be used" to steal its customers' identities. 48 F.4th at 157.

Moreover, it is reasonable to infer that Plaintiffs' data was misused, even though that "is not necessarily required" to plead an injury in fact. *Id.* at 154. Just as CLOP did with

ExecuPharm's data, Rhysida has put Prospect's data up for sale on the dark web. *See id.* at 150. Indeed, Rhysida appears to have gone one step further, "indicat[ing] that they have already sold more than half of the data." In such circumstances, particularly given the reasonable inferences to which Plaintiffs are entitled at this early stage in the litigation, *In re Allergan ERISA Litig.*, 975 F.3d 348, 354 (3d Cir. 2020), even if the Amended Complaint does not expressly allege that Rhysida misused Plaintiffs' data, they plausibly have alleged that their data has been published to the Dark Web, from which the Court "can reasonably assume" that Plaintiffs "face[] a substantial risk of identity theft or fraud," *Clemens*, 48 F.4th at 157. Indeed, "[w]hy else would hackers break into a [company's] database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015). Each of the factors identified in *Clemens* thus favors treating the future injuries that Plaintiffs have alleged as imminent enough to qualify as injuries-in-fact.[4]

On top of these allegations, the actual injuries that Doverspike and Medina identify separately satisfy Article III. Doverspike alleged that she received fraudulent charges "from an entity called 'Midnight Wonders' that she has no affiliation with" just a couple of months after Rhysida posted its dataset on the dark web. Similarly, Medina, who "confirmed that his information was exposed in the breach," has had car and credit card loans taken out in his name, causing his credit score to drop substantially. These Named Plaintiffs have alleged not just imminent, but actual identity theft injuries. *See In re Am. Med. Collection Agency, Inc.*

[4] In this way, *In re Retreat Behavioral Health LLC*, which Prospect relies on as persuasive authority, is distinguishable. There, the district court evaluated allegations that the plaintiffs, victims of a data breach at Retreat, now were subject to "an increased risk of misuse, theft, and fraud." 2024 WL 1016368, at *1 (E.D. Pa. Mar. 7, 2024). They did not allege that their personal information had made it to the dark web and thus failed to allege that their personal data "ha[d] been published or misused in any fashion," so their "complaint relie[d] on mere speculation about what *might* happen in the future. *Id.* at *1, *3. As discussed above, at this stage, Plaintiffs plausibly have alleged publication and misuse.

Customer Data Sec. Breach Litig., 2021 WL 5937742, at *8 (D.N.J. Dec. 16, 2021) ("The fraudulent charges identified by . . . Plaintiffs permit the inference that their specific information has been accessed and misused."); *Norman v. Trans Union, LLC*, 669 F. Supp.3d 351, 371 (E.D. Pa. 2023) (collecting cases that "have found that diminution of credit score confers standing as a financial harm that impacts a consumer's economic condition").

Thus, Plaintiffs' injuries are "actual" or "imminent" as required to confer them Article III standing.

b. Concrete

But to count as injuries-in-fact, they must be concrete as well. "Concrete" injuries are "real, and not abstract." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016) (internal quotation marks and citations omitted). "Central to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms including . . . reputational harm." *TransUnion v. Ramirez*, 594 U.S. 413, 417 (2021) (citation omitted). In data breach cases like this one, the "unauthorized exposure of personally identifying information that results in an increased risk of identity theft or fraud . . is closely related to [the harm caused] by privacy torts that are 'well-ensconced in the fabric of American law.'" *Clemens*, 48 F.4th at 155 (quoting *In re Horizon*, 846 F.3d at 638-39). "Though such an injury is intangible, it is nonetheless concrete." *Id.*

"Where the plaintiff seeks injunctive relief, the allegation of a risk of future harm alone can qualify as concrete as long as it 'is sufficiently imminent and substantial.'" *Id.* (quoting *TransUnion*, 594 U.S. at 435); *see City of Los Angeles v. Lyons*, 461 U.S. 95, 101-02 (1983). But where, as here (in part), a plaintiff presses a claim for damages based on what he or she argues are imminent injuries, Article III demands more for an injury to be considered concrete.

In such suits, "the exposure to the risk of future harm [must] itself cause[] a *separate* concrete harm" to satisfy Article III. *TransUnion*, 594 U.S. at 436. Thus, "in the data breach context, where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms." *Clemens*, 48 F.4th at 155-56. "For example, if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury." *Id.* at 156.

Prospect argues that Plaintiffs have not suffered concrete injuries because the injuries that they allegedly suffered are simply "'mitigation' efforts" that do not satisfy *Clemens*. But *Clemens* did not announce such a rule. The Third Circuit treated "emotional distress and related therapy costs, "the time and money involved in mitigating the fallout of the data breach," and "intangible harms like the disclosure of private information" as sufficient separate concrete harms under *TransUnion*. *Clemens*, 48 F.4th at 158-59.[5] Each Named Plaintiff alleges injuries along these lines, so for each of them, the risk of identity theft that they identify is sufficiently concrete to satisfy Article III with respect to both their claims for equitable relief and damages.

Each Named Plaintiff has plausibly alleged that his or her injuries are concrete and thus has suffered an injury in fact.

ii. Traceability

The next requirement for Article III standing is that the injury in fact be "fairly traceable to" the defendant's conduct, *Davis v. Wells Fargo*, 824 F.3d 333, 347 (3d Cir. 2016), "as

[5] And even if that were the rule that *Clemens* had announced, it would not dispose of Plaintiffs' Amended Complaint, as many of Plaintiffs' alleged injuries, such as the fraudulent transactions that Doverspike and Medina allegedly suffered, cannot reasonably be considered solely mitigation related.

opposed to an independent action of a third party," *Clemens*, 48 F.4th at 158 (citing *Lujan*, 504 U.S. at 560). Either but-for causation or concurrent causation can establish a legally sufficient relationship between the injury-in-fact and the challenged conduct. *Clemens*, 48 F.4th at 158. "[M]ere speculation," on the other hand, does not suffice. *Clapper*, 568 U.S. at 410.

Here again, *Clemens* points the way. In that case, the plaintiff's allegations that the defendant had "fail[ed] to safeguard her information," which "enabled CLOP to publish it on the Dark Web as part of the stolen dataset" provided the necessary causal link to confer Article III standing with respect to her alleged substantial increased risk of falling victim to identity theft or fraud. *Clemens*, 48 F.4th at 158. Plaintiffs' allegations here are nearly identical. According to the Amended Complaint, Prospect "fail[ed] to implement adequate data security measures and protocols to properly safeguard and protect" data in its custody "from a foreseeable cyberattack." That failure led to its publication on the dark web, as detailed above.

Prospect contends that Plaintiffs' injuries were "isolated events" that "are facially unrelated to" the company's conduct "besides a tenuous temporal proximity." Thus, per Prospect, "Plaintiffs fail to allege that their data was taken or even misused *because* of the [d]ata [b]reach." But the Amended Complaint describes a plausible causal link between Prospect's conduct and Plaintiffs' injuries. In late July or early August of 2023, the company suffered a data breach. Prospect's data appeared *en masse* on the dark web later in August. It is reasonable to infer that this included Plaintiffs' personal information. At this early stage in the litigation, that is all that is needed to plead traceability.[6] *Id.*

[6] Prospect argues in its reply brief that Plaintiffs' failure to allege "that their information was otherwise kept secure" or "that they have not received other notice letters about the same information from other companies who may have experienced data breaches" is "fatal." Even if not forfeited, *Laborers' Int'l Union of N. Am. v. Foster Wheeler Corp.*, 26 F.3d 375, 398 (3d Cir. 1994), this argument is presented without legal support and cannot be credited. *See Reynolds v. Wagner*, 128 F.3d 166, 178 (3d Cir. 1997) ("[A]n argument consisting of no more than a conclusory assertion such as the one made here . . . will be deemed waived."); *see* E.D. Pa. Local Civ. R. 7.1(c).

In sum, at least one Named Plaintiff (indeed, more than one) has plausibly alleged that they have suffered an injury in fact, and that those injuries can fairly be traced to Prospect's conduct. *Lujan*, 504 U.S. at 560. As Prospect does not contest that their injuries would be redressed by the relief Plaintiffs seek, *id.* at 561, they therefore plausibly have alleged Article III standing.

B. The Plausibility of Plaintiffs' Claims

That said, Prospect moves to dismiss each of the claims included in the Amended Complaint. Fed. R. Civ. P. 12(b)(6).

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* When analyzing a motion to dismiss, the complaint must be construed "in the light most favorable to the plaintiff," with the question being "whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." *Fowler*, 578 F.3d at 210. Well-pleaded facts are taken as true, and a determination is made as to whether those facts state a "plausible claim for relief." *Id*. at 210-11.

On a motion to dismiss, a complaint may be dismissed with prejudice and plaintiff may be denied leave to further amend his claims "if amendment would be inequitable or futile." *Grayson v. Mayview State Hosp.*, 293 F.3d 103, 108 (3d Cir. 2002). "'Futility' means that the complaint, as amended, would fail to state a claim upon which relief could be granted." *Shane v. Fauver*, 213 F.3d 113, 115 (3d Cir. 2000). Simply stated, a court may dismiss a claim with

prejudice if an amendment would still not cure the deficiency. *Id.* Where, as here, one amended pleading already has been filed, further amendment may be allowed "only with the opposing party's written consent or the court's leave. The court should freely give leave when justice so requires." Fed. R. Civ. P. 15(a)(2). That means that "leave to amend generally must be granted unless the amendment would not cure the deficiency." *Shane*, 213 F.3d at 115; *accord Phillips v. County of Allegheny*, 515 F.3d 224, 234 (3d Cir. 2008).

i. Negligence

To state a claim for negligence, Plaintiffs must plausibly allege: "(1) a duty or obligation recognized by law; (2) a breach of that duty; (3) a causal connection between the conduct and the resulting injury; and (4) actual damages." *Toro v. Fitness Int'l LLC*, 150 A.3d 968, 976-77 (Pa. Super. 2016) (citation omitted); *accord Thomas v. Stenberg*, 206 Cal. App.4th 654, 662 (Cal. App. 2012).[7] Prospect argues that Plaintiffs' negligence claim does not satisfy the last two elements of the *prima facie* case. Per Prospect: (1) "besides a tenuous temporal proximity," the Amended Complaint is bereft of plausible allegations of a causal nexus between the data breach and the injuries alleged; and, (2) those injuries are only "isolated events of allegedly suspicious activity" that do not count as "actual damages"—things like credit card fraud or improperly paid taxes.[8]

Both arguments fail. "[T]o to demonstrate actual or legal causation, the plaintiff must show that the defendant's act or omission was a 'substantial factor' in bringing about the injury."

[7] The parties use both California and Pennsylvania law to advance their arguments. Obviously, as to Plaintiffs' statutory and constitutional claims under California law, that state's substantive law governs. And as to the parties' common-law claims, neither Plaintiffs nor Prospect identifies any true conflicts between the states' laws. Therefore, in analyzing Prospect's Motion to Dismiss those claims, California and Pennsylvania law are both consulted. *See Hutton Grp., Inc. v. Advantage Mktg. Int'l, Inc.*, 2010 WL 3938248, at *5 (W.D. Pa. Oct. 5, 2010).

[8] Prospect thus does not contest that the Amended Complaint plausibly alleges that the company owed Plaintiffs a duty to safeguard their personal information or that, because of the cyberattack, it breached that duty.

Saelzler v. Advanced Grp. 400, 23 P.3d 1143, 1150 (Cal. 2001); *accord Hamil v. Bashline*, 392 A.2d 1280, 1284 (Pa. 1978). In data breach cases like this one, "allegations that Plaintiffs provided Defendant with their PII and PHI, and that because of the breach, their information was available and thereafter placed on a ransomware website on the dark web" have been found to plausibly plead causation in negligence claims. *Opris v. Sincera Reproductive Med.*, 2022 WL 1639417, at *6 (E.D. Pa. May 24, 2022). Even courts that have articulated more stringent standards "have found plausible causation exists between plaintiffs' injury and defendant's failure to safeguard plaintiffs' PII" where the complaint alleges that: (1) "their PII was exposed in a data breach;" and, (2) "they suffered unauthorized access notifications, fraudulent bank activity, and time losses in mitigating such injury." *Kirsten v. Cal. Pizza Kitchen, Inc.*, 2022 WL 16894503, at *8 (C.D. Cal. July 29, 2022) (citing *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp.3d 1130, 1142 (C.D. Cal. 2021)). Allegations of unwanted online interactions "common in daily life without a data breach," on the other hand, are insufficient to plead causation. *Id.*

Here, the allegations in the Amended Complaint clear even the higher bar set in *Kirsten*. Plaintiffs allege that Prospect was the victim of a data breach that led to the publication of personal identifiable information and patient files on the dark web. Some of the Named Plaintiffs, such as Rodney Hoggro, Latoya Pratcher, and Fidel Medina, allege that their personal information in fact was exposed through this breach, and given the size of the datasets posted on the dark web by Rhysida, it is reasonable at the motion-to-dismiss stage to infer that the remaining Named Plaintiffs' information, who received "Notice[s] of [a] Security Incident" from Prospect, suffered the same fate. After the data breach, Plaintiffs all allegedly spent time dealing with its consequences, and, as discussed *supra*, many suffered actual financial losses as a result. Because none of these incidents is "common in daily life without a data breach," *id.*, under any

standard that the parties have identified, the Amended Complaint plausibly alleges causation as required for the *prima facie* case of negligence.

And with respect to damages, the injuries that Plaintiffs allege have an established pedigree in tort cases arising out of data breaches. Courts in both California and Pennsylvania "have found that 'injury by way of costs relating to credit monitoring, identity theft protection, and penalties' can 'sufficiently support a negligence claim.'" *Huynh v. Quora, Inc.*, 508 F. Supp.3d 633, 650 (N.D. Cal. 2020) (quoting *Corona v. Sony Pictures Ent., Inc.*, 2015 WL 3916744, at *4-5 (C.D. Ca. June 15, 2015)) (collecting cases); *see Opris*, 2022 WL 1639417, at *7.

Here, contrary to Prospect's argument, the Amended Complaint alleges that all Plaintiffs suffered various injuries arising out of the data breach, including "financial costs incurred mitigating the materialized risk and imminent threat of identity theft" and "financial costs incurred due to actual identity theft." These are recognized forms of damages in data breach cases. Therefore, Plaintiffs have plausibly alleged they suffered cognizable tort damages, and their negligence claim will not be dismissed.

***ii. Negligence* Per Se**

Plaintiffs also maintain a separate count alleging negligence *per se* under the theory that Prospect's alleged lax protection of their personal information violated Section Five of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce." 15 U.S.C. § 45(a)(1).

Under both California and Pennsylvania law, negligence *per se* is not a freestanding tort. *In re Accellion, Inc. Data Breach Litig.*, 2024 WL 333893, at *9 (N.D. Cal. Jan. 29, 2024); *Kovalev v. Lidl US, LLC*, 647 F. Supp.3d 319, 346 (E.D. Pa. 2022). Instead, it "establish[es] a presumption of negligence for which the [violation of a] statute serves the subsidiary function of providing evidence of an element of a preexisting common law cause of action." *Quiroz*

v. Seventh Ave. Ctr., 140 Cal. App.4th 1256, 1285-86 (Cal. App. 2006); *accord Mahan v. Am-Gard, Inc.*, 841 A.2d 1052, 1058 (Pa. Super. 2003) ("The concept of 'negligence *per se*' establishes the elements of duty and breach of duty where an individual violates an applicable statute, ordinance, or regulation designed to prevent a public harm."). In both states, the violation of some—but not all—statutes give rise to that presumption. A plaintiff must further prove that: (1) "the violation proximately caused injury;" (2) "the injury resulted from an occurrence the enactment was designed to prevent;" and, (3) "the plaintiff was a member of the class of persons the statute was intended to protect." *Safari Club Int'l v. Rudolph*, 862 F.3d 1113, 1126 (9th Cir. 2017) (citation omitted); *accord Congini ex rel. Congini v. Portersville Valve Co.*, 470 A.2d 515, 517-18 (Pa. 1983) (citing Restatement (Second) of Torts § 286) (Am. L. Inst. 1965)).

Prospect argues that this separate count must be dismissed for multiple reasons. First, because previous district courts have remarked that "[w]here a plaintiff alleges negligence and negligence per se as separate causes of action, courts within the Third Circuit routinely dismiss the negligence per se claim as subsumed within the standard negligence claim," *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp.3d 514, 531 (M.D. Pa. 2021) (collecting cases), the same should happen here. While that is true, this does not address the viability of Plaintiffs' theory of liability more broadly. If the allegations supporting an ordinary negligence theory and a negligence *per se* both are plausible, there is every reason to allow discovery on both theories. The proper remedy here is not dismissal of negligence *per se* as a theory, but simply dismissal of any separate count in the operative complaint. *Weinberg v. Legion Athletics, Inc.*, 683 F. Supp.3d 438, 452 (E.D. Pa. 2023) ("We will dismiss Mr. Weinberg's negligence per se claim but will permit him to pursue a negligence per se theory as part of his negligence claim."); *see also*

In re Rutter's, 511 F. Supp.3d at 531-32; *Kirsten*, 2022 WL 16894503, at *9.

Prospect next argues that, even if theoretically available, negligence *per se* is not a viable theory here because Plaintiffs premise it on a law, the FTC Act, that does not include a private right of action. True enough, the FTC Act is not subject to private enforcement, *Sandoz Pharms. Corp. v. Richardson-Vicks, Inc.*, 902 F.2d 222, 231 (3d Cir. 1990), but neither Pennsylvania nor California courts require a private right of action be available for a statute to serve as the hook for a negligence *per se* theory, *Cabiroy v. Scipione*, 767 A.2d 1078, 1081 (Pa. Super. 2001) ("We conclude that although no private cause of action is set forth in the [Food, Drug, and Cosmetic] Act, it was certainly designed to protect a particular class of individuals . . . ."); *Sierra-Bay Fed. Land Bank Ass'n v. Sup. Ct.*, 227 Cal. App.3d 318, 332-33 (Cal. App. 1991) (noting that, when a statute is violated, "it is the tort of negligence, and not the violation of the statute itself, which entitles a plaintiff to recover civil damages"). There is no categorical bar against negligence *per se* claims premised on such statutes. Instead, the absence of a private right of action "is just an indicator or a factor to consider . . . . A statute may still be used as the basis for a negligence *per se* claim when it is clear that, despite the absence of a private right of action, the policy of the statute will be furthered by such a claim because its purpose is to protect a particular group of individuals." *Sharp v. Artifex, Ltd.*, 110 F. Supp.2d 388, 392 (W.D. Pa. 1999); *see Wagner v. Anzon, Inc.*, 684 A.2d 570, 629-30 (Pa. Super. 1996).

The question, then, is "whether the purpose of the" FTC Act "is to protect the interest of a group of individuals, as opposed to the general public." *Cabiroy*, 767 A.2d at 1081. And where the plaintiffs have adequately pleaded that they are part of the class that the FTC Act is designed to protect, courts applying state negligence *per se* doctrines of similar sweep have allowed these claims to proceed. *See Carr v. Okla. Student Loan Auth.*, 2023 WL 6929853, at *4

(W.D. Okla., Oct. 19, 2024) (Oklahoma); *Kirsten*, 2022 WL 16894503, at *9 (California); *In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp.3d 447, 478-79 (D. Md. 2020) (Georgia); *cf. In re Blackbaud, Inc., Customer Data Breach Litig.*, 567 F. Supp.3d 667, 684-85 (D.S.C. 2021) (South Carolina) (granting defendant's motion to dismiss where plaintiffs failed to "explain the parameters of" the "class the FTC Act was designed to protect").[9] Here, Plaintiffs allege that they are "consumers" and thus fall "within the class of persons" the law "was meant to protect." Considering this pleading and the weight of this persuasive authority, and because "a decision in favor of [Prospect] on this point would not dispose of [Plaintiffs'] underlying negligence claim," the appropriate decision is to defer judgment of the viability of the FTC Act as a hook for negligence *per se* to summary judgment. *In re Rutter's*, 511 F. Supp.3d at 532; *accord Opris*, 2022 WL 1639417, at *10 (citing *In re Wawa, Inc. Data Sec. Litig.*, 2021 WL 1818494, at *7 (E.D. Pa. May 6, 2021)).

Prospect's Motion to Dismiss therefore will be granted with respect to Plaintiffs' separate count alleging negligence *per se*, but Plaintiffs may press it as a theory to support their negligence claim and may rely on Prospect's alleged violation of the FTC Act in doing so.

iii. Breach of Implied Contract

Under both Pennsylvania and California law, a breach of contract claim requires proof of: "(1) the existence of a contract, including its essential terms, (2) a breach of a duty imposed by the contract[,] and (3) resultant damages." *Ware v. Rodale Press, Inc.*, 322 F.3d 218, 225 (3d Cir. 2003) (quoting *CoreStates Bank, N.A. v. Cutillo*, 723 A.2d 1053, 1058 (Pa. Super. 1999)); *accord First Com. Mortg. Co. v. Reece*, 89 Cal. App.4th 731, 745 (Cal. App. 2001). "A cause of

[9] The cases on which Prospect relies are inapposite because they apply the law of states, such as New York and Florida, that require that a private right of action be available in the underlying statute for a negligence *per se* claim to be maintained. *In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *10 (S.D.N.Y. Aug. 4, 2021); *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *9 (M.D. Fla. Jan. 27, 2020).

action for breach of implied contract has the same elements as does a cause of action for breach of contract, except that the promise is not expressed in words but is implied from the promisor's conduct." *Gomez v. Lincare, Inc.*, 173 Cal. App.4th 508, 526 (Cal. App. 2009); *accord Liss & Marion, P.C. v. Recordex Acquisition Corp.*, 983 A.2d 652, 659, 661 (Pa. 2009); *In re Rutter's*, 511 F. Supp.3d at 533-34 (citation omitted).

Plaintiffs allege that they "entered into implied contracts with [Prospect] under which [it] agreed to safeguard and protect [their private] information and to timely and accurately notify" them when "their information had been breached and compromised." Prospect, despite having "accept[ed]" Plaintiffs' personal information "and payment for services," breached that implied contract "by failing to take reasonable measures to safeguard [Plaintiffs'] [p]rivate [i]nformation."

Prospect argues that Plaintiffs have failed to state a claim for breach of an implied contract because they contend that the mere requirement that customers share their personal information with a defendant does not give rise to an implied contract. Indeed, the Third Circuit has ruled in a non-precedential opinion that such an allegation, standing alone, "d[oes] not create a contractual promise to safeguard that information, especially from third party hackers." *Longenecker-Wells v. Benecard Servs., Inc.*, 658 F. App'x 659, 662 (3d Cir. 2016) (not precedential). In that its reasoning is persuasive, in line with several district courts in this circuit, the Court will adopt its' conclusion here. *Longenecker-Wells* has been applied to find that an implied contract exists where the defendants say that they will "take[] security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction" of their data and "reference[] company-specific documents and policies to support a promise

implied by the parties' conduct."[10] *In re Rutter's*, 511 F. Supp.3d at 535.

Here, Plaintiffs do not point to any company policy or other statement plausibly indicating that Prospect promised that their personal information would be safeguarded. Instead, Plaintiffs allege that: (1) "accepting [their] information and payment for services;" and, (2) "specific industry data security standards and FTC guidelines on data security" gave rise to that promise. As to the first of these sources, *Longenecker-Wells* forecloses the possibility that this conduct, without more, could give rise to an implied contract between Plaintiffs and Prospect: there, as here, the "requirement" that Plaintiffs hand over their sensitive data in exchange for healthcare "alone did not create a contractual promise to safeguard that information." 658 F. App'x at 662. As to the second, Plaintiffs point the Court to no authority holding that an "industry data security standard[]" or federal regulation can be treated as a statement from a defendant, let alone one by which it "implicitly assent[ed] to a contract to protect Plaintiffs' Personal Information." *In re Am. Med. Collection Agency*, 2021 WL 5937742, at *20. Thus, Plaintiffs fail to plausibly plead the existence of an implied contract between them and Prospect to safeguard their personal information, and their claim seeking to enforce such a contract will be dismissed without prejudice.

iv. Common-Law Invasion of Privacy and Violation of the California Constitution

A common-law invasion of privacy claim under Pennsylvania law is available against

[10] *Accord Tjahjono v. Westinghouse Air Brake Techs. Corp.*, 2024 WL 1287085, at *7 (W.D. Pa. Mar. 26, 2024) (denying a motion to dismiss a breach of implied contract claim where plaintiffs "quote language from [defendant's] notification of the data breach recognizing its responsibility to protect employees' PII"); *Bray v. GameStop Corp.*, 2018 WL 11226516, at *6 (D. Del. Mar. 16, 2018) (denying a motion to dismiss in reliance on defendant's privacy policy, "which suggests an acknowledgment that data security was known by both sides to be an important factor in using a credit or debit card to make purchases"); *cf. In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *20 (D.N.J. Dec. 16, 2021) ("[T]he same privacy notices cited by Plaintiffs also explicitly state that Defendants *did not* ensure the privacy and safety of Plaintiffs' information. . . . These statements make doubly clear that Defendants did not implicitly assent to a contract to protect Plaintiffs' Personal Information.").

"[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." *Kline v. Sec. Guards, Inc.*, 386 F.3d 246, 260 (3d Cir. 2004) (quoting *Harris v. Easton Publ'g Co.*, 483 A.2d 1377, 1383 (Pa. Super. 1984)). California law requires the like to establish the common-law tort. *In re Ambry*, 567 F. Supp.3d at 1143. To prevail on a lawsuit brought under Article I, Section 1 of California's Constitution,[11] which provides that: "[a]ll people are by nature free and independent and have inalienable rights. Among these are . . . privacy," Cal. Const. art. I, § 1, a plaintiff must prove "'a legally protected privacy interest,' 'a reasonable expectation of privacy in the circumstances,' and 'conduct by defendant constituting a serious invasion of privacy.'" *In re Sequoia Benefits and Ins. Data Breach Litig.*, 2024 WL 1091195, at *5 (N.D. Cal. Feb. 22, 2024) (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633, 657 (Cal. 1994)).

All of Plaintiffs' privacy claims fail for the same reason: the Amended Complaint does not allege that *Prospect*, as opposed to *Rhysida*, intentionally intruded on information in which Plaintiffs had a reasonable expectation of privacy, as necessary to win relief. *Kline*, 386 F.3d at 260; *Marich v. MGM/UA Telecomms., Inc.*, 113 Cal. App.4th 415, 421 (Cal. App. 2003); *In re Sequoia*, 2024 WL 1091195, at *5; *see O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989) ("[T]he intrusion, as well as the action, must be intentional."). In data breach cases, courts routinely have held that the hacker's intentional intrusion should not be attributed to the defendant custodian of the plaintiffs' personal information[12] unless the defendant at least

[11] Prospect argues that this provision of the California Constitution does not contain a private right of action for damages. Because Plaintiffs have not stated a claim under that provision regardless, the Court assumes *arguendo* that a private right of action is available and does not directly address this argument.

[12] *In re Sequoia*, 2024 WL 1091195, at *6 (collecting cases); *accord In re Am. Med. Collection Agency*, 2023 WL 8540911, at *7 (D.N.J. May 5, 2023) ("Plaintiffs have not alleged that Defendants disclosed their private information to hackers. Neither have Plaintiffs alleged facts suggesting that when Defendants shared information

recklessly, *Fagan v. City of Vineland*, 22 F.3d 1296, 1324 (3d Cir. 1994), failed to safeguard or in fact disclosed the plaintiffs' personal information.[13]

Here, the Amended Complaint merely accuses Prospect of, at most, negligence in how it handled Plaintiffs' personal information. Unlike Rhysida, which is accused of having conducted the cyberattack and stolen Plaintiffs' data, Prospect is alleged to have merely "fail[ed] to implement adequate data security measures and protocols to properly safeguard and protect" that data, which led to "a foreseeable cyberattack on its systems that resulted in [its] unauthorized access and theft." Plaintiffs' allegation that Prospect "intentionally configured [its] systems in such a way that stored [their] personal information to be left vulnerable to malware/ransomware attack"—assuming *arguendo* that it is non-conclusory, *Iqbal*, 556 U.S. at 678—does not move the needle either. Prospect's "configuring" of their data security systems is not the conduct that must be proven to be intentional in an invasion of privacy claim. The defendant's state of mind with respect to the "intru[sion]" is what matters. *Kline*, 386 F.3d at 260. Only Rhysida is plausibly alleged to have intentionally intruded on anyone's privacy.[14]

---

with AMCA, they did so with the intent to invade Plaintiff's privacy."); *Kirsten*, 2022 WL 16894503, at *4 ("Plaintiffs have not provided anything specific regarding whether or how Defendant knew its security was deficient or any other allegations indicating that Defendant intentionally allowed unauthorized access to Plaintiffs' [private information]. Plaintiffs thus provide only conclusory allegations regarding intentional invasion of privacy . . . ."); *In re Brinker*, 2020 WL 691848, at *22 ("But Brinker did not do any act that made Plaintiffs' information known—the information was stolen by third-parties. Even assuming, *arguendo*, that Brinker's inadequate security facilitated the theft, such a claim would lie in negligence not breach of confidence.").

[13] *See, e.g.*, *Savidge v. Pharm-Save, Inc.*, 2021 WL 3076786, at *3-4 (W.D. Ky. July 1, 2021) (denying a motion to dismiss an invasion of privacy claim based on intrusion upon seclusion where the defendant "was aware of the potential hazard for phishing schemes as outlined in [an] IRS Warning," "failed to provide training or establish policies and procedures for protecting personal and sensitive information of its employees," and "one or more [of its] agents . . . released the sensitive and personal information in the W-2s to third-party cybercriminals" because that conduct constituted "such reckless disregard for the privacy of the plaintiff that the actions rise to the level of being an intentional tort" (quoting *McKenzie v. Allconnect, Inc.*, 369 F. Supp.3d 810, 819 (E.D. Ky. 2019))).

[14] *In re Ambry*, in which the district court noted that "[c]ourts have refused to dismiss invasion of privacy claims at the motion to dismiss stage where, as here, a data breach involved medical information, because the disclosure of such information is more likely to constitute an 'egregious breach of the social norms' that is 'highly offensive,'" and on which Plaintiffs rely heavily, is not to the contrary. 567 F. Supp.3d at 1143. There, the court was remarking on the unrelated requirement that the intrusion be highly offensive to a reasonable person. Indeed, in the many data

Because the Amended Complaint does not allege intentional conduct by Prospect itself, Plaintiffs' common-law and constitutional invasion of privacy claims will be dismissed with prejudice.

v. Violation of the California Confidentiality of Medical Information Act

The next count in the Amended Complaint alleges a violation of two separate provisions of the CMIA: Section 56.101(a), and Section 56.36(b).

Section 56.101(a) contains two sentences. First, it establishes a duty: "Every provider of health care . . . who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101(a). Next, it lays out the consequences for breaching that duty: "Any provider of health care . . . who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." *Id.* Section 56.36(b), on which Plaintiffs rely here, in turn, says that "In addition to any other remedies available at law, an individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of" nominal damages worth $1,000 or "actual damages, if any, sustained by the patient." *Id.* § 56.36(b).[15]

As the California Court of Appeal has observed, these two statutory sections use different verbs: Section 56.101(a) imposes a duty to properly "maintain[]" and "preserve[]" patients' medical records, while Section 56.36(b) provides for damages for "negligently releas[ing]" that

---

breach cases involving medical information, that is likely to be the case. It does not bear, however, on how to analyze the separate element requiring that the intrusion be intentional.

[15] The Amended Complaint's count alleging violation of the CMIA also alleged that Prospect violated Section 56.10(a) of the law, but Plaintiffs have withdrawn that claim.

information. These words "are not synonymous." *Regents of Univ. of Cal. v. Super. Ct.*, 220 Cal. App.4th 549, 564 (Cal. App. 2013). Although "releas[ing]" data does not require "an affirmative communicative act by the health care provider," *id.* at 553, it does require that that provider's substandard maintenance or preservation "result[] in unauthorized or wrongful access to the information," *id.* at 554; *see Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp.3d 898, 923 (S.D. Cal. 2020). Thus, "[n]o breach of confidentiality"—and no liability under Section 56.36(b)—"takes place until an unauthorized person views the medical information." *Sutter Health v. Super. Ct.*, 227 Cal. App.4th 1546, 1557-58 (Cal. App. 2014). "While loss of possession [of medical information] may result in breach of confidentiality, loss of possession does not necessarily result in a breach of confidentiality." *Id.*

Prospect argues that Plaintiffs' CMIA claim should be dismissed for two reasons. First, the company submits that Plaintiffs have failed to plausibly allege "that purported negligence by [the company] . . . caused a third party to access and view their medical information. Instead, Plaintiffs allege only that PII changed hands," not that it has been improperly "viewed or accessed"—*i.e.*, "released," as California courts have interpreted Section 56.36(b). Second, any information that was exposed was not "medical information"[16] that it had a duty to protect under

[16] The CMIA defines "medical information" as:

> [A]ny individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, reproductive or sexual health application information, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.

Cal. Civ. Code § 56.05(j).

Section 56.101(a).[17]

But these arguments are belied by the allegations in the Amended Complaint. As to Prospect's first argument, Plaintiffs allege that Rhysida not only had posted this data on the Dark Web, but also that the group indicated that it had "already sold more than half of" it. On top of that, Prospect's own Notice Letter conceded that whoever penetrated its system "accessed and/or acquired files that contain information pertaining to certain Prospect Medical employees and dependents." In such circumstances, it is more than reasonable to infer that Plaintiffs' personal information had been wrongfully viewed or accessed.[18] *Regents*, 220 Cal. App.4th at 554.

As to Prospect's second argument, Plaintiffs allege that the data breach exposed, among other things, their "diagnosis information, lab results, prescription information, [and] treatment information." And Rhysida bragged that "patient files (profile, medical history)" were for sale on the dark web. It is plausible to infer that this information therefore constituted "individually identifiable information . . . regarding a patient's medical history" and thus "medical information." Cal. Civ. Code § 56.05(j).

Thus, Prospect's Motion to Dismiss will be denied with respect to Plaintiffs' CMIA claim.

---

[17] Prospect also argues that Plaintiffs have not shown "that they are entitled to relief for any negligence by Prospect, let alone negligence [that] resulted in their medical information being viewed or accessed." But as discussed above, Plaintiffs plausibly have alleged exactly that in the negligence count of their Amended Complaint.

[18] *See, e.g.*, *Stasi*, 501 F. Supp.3d at 924 (concluding that, where the defendant was alleged to have "posted [plaintiffs'] information on the internet, making it searchable, findable, viewable, printable, copiable, and downloadable by anyone in the world with an internet connection, . . . it can be reasonably inferred that someone viewed it"); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp.3d 1284, 1299 (S.D. Cal. 2020) (inferring that plaintiffs' data had been wrongfully viewed based on "complaint letters they received from" the defendant "indicating that their information was exposed" and "an increase in medical-related spam emails and phone calls"); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp.3d 1183, 1202 (D. Or. 2016) (inferring wrongful viewing where plaintiff allegedly had "received a letter from Premera notifying her that her personal information may have been compromised" and "discovered on her credit report an inquiry for a car loan that she did not recognize and that her checking account was fraudulently accessed around the same time").

vi. Violation of the California Unfair Competition Law

The last count to be addressed is Plaintiffs' allegation that Prospect violated California's Unfair Competition Law ("UCL"), which "prohibits, and provides civil remedies for, unfair competition, which it defines as 'any unlawful, unfair or fraudulent business act or practice.'" *Kwikset Corp. v. Super. Ct.*, 246 P.3d 877, 883 (Cal. 2011) (quoting Cal. Bus. & Prof. Code § 17200). "Unlawful," "unfair" and "fraudulent" conduct are "three varieties of unfair competition." *Cal-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 973 P.2d 527, 548 (Cal. 1999) (citation omitted).

In the Amended Complaint, Prospect is alleged to have engaged in "unfair" conduct by (1) "fail[ing] to implement and maintain reasonable security measures to protect Plaintiffs' . . . personal information from unauthorized disclosure;" (2) "fail[ing] to identify foreseeable security risks" and "remediate" them "following previous cybersecurity incidents and known coding vulnerabilities in the industry;" (3) [m]isrepresenting that it would protect the privacy and confidentiality of Plaintiffs' . . . personal information;" and, (4) "[o]mitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure" that information. Plaintiffs also allege that Prospected engaged in "unlawful" conduct by violating: (1) the California Customer Records Act, Cal Civ. Code §§ 1798.81.5, 1798.82; (2) the CMIA, *id.* § 56; (3) the California Consumer Legal Remedies Act, *id.* § 1780 *et seq.*; (4) Section Five of the FTC Act, 15 U.S.C. § 45; and, (5) California common law.

Before reaching the merits of Plaintiffs' claim, an additional requirement for standing must be addressed here. The private right of action to enforce the UCL has been "limited to any person who has suffered injury in fact and has lost money or property as a result of unfair competition." *Kwikset*, 246 P.3d at 884 (internal quotation marks and citations omitted). That means that, to have standing, a plaintiff must: "(1) establish a loss or deprivation of money or

property sufficient to qualify as injury in fact, *i.e.*, *economic injury*, and (2) show that that economic injury was the result of, *i.e.*, *caused by*, the unfair business practice or false advertising that is the gravamen of the claim." *Id.* at 885; *see* Cal. Bus. & Prof. Code § 17204. As the Supreme Court of California has explained:

> There are innumerable ways in which economic injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.

Kwikset, 246 P.3d at 885-86.

Prospect argues that, whether or not Plaintiffs have satisfied Article III's requirements, they do not have standing to bring a UCL claim because they have not "actually allege[d] what money or property they have lost." But the allegations in the Amended Complaint suffice to grant Plaintiffs standing on this claim. They allege that they "overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not." This "benefit-of-the-bargain" theory of injury is an accepted basis for establishing standing to bring a UCL claim. *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp.3d 1284, 1301 (S.D. Cal. 2020). Here, as in *Solara*, Plaintiffs "acquired less in their transactions . . . than they would have if [Prospect] had sufficiently protected their Personal Information." *Id.*; *see also In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp.3d 1197, 1224 (N.D. Cal. 2014); *Kwikset*, 246 P.3d at 885. Thus, Plaintiffs have standing to sue under the UCL, and Prospect's Motion will not be granted on this ground.[19]

[19] For the first time in its Reply, Prospect argues that dismissal is proper because Plaintiffs "fail to articulate . . . any 'bargain struck' between Prospect and the Plaintiffs (as opposed to their health insurance provider)." This argument is forfeited. *Laborers' Int'l Union of N. Am.*, 26 F.3d at 398. And even if it were properly before the Court, it would not change the result here, as each Named Plaintiff alleges that they "obtained services" from Prospect that were "intended to be accompanied by adequate data security . . . but [were] not." They thus "did not get what they

That said, because the Amended Complaint contains no allegation that Plaintiffs lack an adequate remedy at law, their UCL claim will be dismissed without prejudice. Plaintiffs seek, among other things, "all monetary . . . relief allowed by law," "restitution of all profits stemming from Defendant's unfair and unlawful business practices," and "other appropriate equitable relief" as redress for Prospect's alleged UCL violations. But "[r]emedies under the UCL are limited to restitution and injunctive relief, and do not include damages." *In re Ambry*, 567 F. Supp.3d at 1147. Thus, "[a] plaintiff 'must establish that she lacks an adequate remedy at law before securing equitable restitution for past harm under the UCL.'" *Id.* (quoting *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020)).

Prospect argues that Plaintiffs' failure to plead that they lack an adequate remedy at law dooms their claim. But *Sonner* arose from a case where the plaintiff, despite her claims having survived motions to dismiss and for summary judgment, sought leave to amend to drop a related damages claim and proceed only with a claim for restitution under the UCL. 971 F.3d at 838. Because of the procedural posture that it arose in, district courts generally have held that *Sonner* does not require UCL plaintiffs to choose between legal and equitable remedies at the motion to dismiss stage. *In re Natera Prenatal Testing Litig.*, 664 F. Supp.3d 995, 1012-13 (N.D. Cal. 2023) (collecting cases). Instead, merely alleging that legal remedies are "not as certain as equitable remedies" can suffice, *id.* at 1012 (quotation omitted), allowing "the Court [to] reassess" the appropriateness of the UCL claim "at a later stage of this case," while "declin[ing] to trim out Plaintiff's equitable restitution claim at this early stage,'" *Nacarino v. Chobani, LLC*, 668 F. Supp.3d 881, 897 (N.D. Cal. 2022) (quoting *Jeong v. Nexo Fin. LLC*, 2022 WL 174236,

paid for and agreed to." At the motion-to-dismiss stage, as buttressed by the additional non-conclusory allegations in the Amended Complaint, that is sufficient to allege a bargain with Prospect as necessary to proceed under a benefit-of-the-bargain theory.

at *27 (N.D. Cal. Jan. 19, 2022)).

Here, however, the Amended Complaint contains no allegations regarding the viability of Plaintiffs' remedies at law, so it cannot be characterized even as pleading in the alternative. *See Sonner*, 971 F.3d at 844 (citing *O'Shea*, 414 U.S. at 502). Instead, it merely alleges that Plaintiffs "were injured and lost money or property, which would not have occurred but for the unfair and unlawful acts alleged." Therefore, Plaintiffs' UCL claim will be dismissed without prejudice with opportunity to plead that they lack an adequate remedy at law.

III. CONCLUSION

For the foregoing reasons, Prospect's Motion to Dismiss will be granted in part and denied in part. An appropriate order follows.

BY THE COURT:

/s/Wendy Beetlestone, J.

WENDY BEETLESTONE, J.